ACTA ARITHMETICA
150.3 (2011)

On a ternary quadratic form over primes

by

Étienne Fouvry (Orsay) and Igor E. Shparlinski (Sydney)

1. Introduction

1.1. Motivation and general notations. Let $Q = Q(X, Y, Z)$ be a ternary quadratic form with integral coefficients. Also, throughout this paper, the letter p, with or without indices, is reserved for prime numbers. Here we address the following question:

What are the multiplicative properties of the multiset $\{Q(p_1, p_2, p_3)\}$*?*

The most natural example of such a Q is $Q(X, Y, Z) = X^2 + Y^2 + Z^2$. It is conjectured that every sufficiently large integer $N \equiv 3 \bmod 24$ with $5 \nmid N$ can be written in the form $N = p_1^2 + p_2^2 + p_3^2$. This conjecture, if true, would lie very deep. The most advanced results in the direction of its proof can be listed according to two points of view. The first one has been initiated by Blomer and Brüdern (see [2, Theorem 1.1] and also [1, Proposition 3.1]) who proved that every N, as above, is of the form $N = n_1^2 + n_2^2 + n_3^2$, where all the prime divisors of n_i are greater than $N^{1/567}$. This result is based on sieve techniques and on bounds of Fourier coefficients of cusp forms, which naturally appear in the theory of quadratic forms (see [1] for a survey).

The second direction starts with Hua [16] in 1938. By the circle method, he proved that almost every N as above can be expressed as the sum of three squares of primes, with, roughly speaking, the expected order of magnitude for the number of representations. Hua's result is an example of Waring–Goldbach problems (see [17] for an introduction to this problem and [12] for more precise results). In Hua's proof, the circle method is essential since, more or less, we are led to count the number of solutions of the equation

$$p_1^2 + p_2^2 + p_3^2 - p_4^2 - p_5^2 - p_6^2 = 0 \quad (p_i \le x).$$

2010 *Mathematics Subject Classification*: Primary 11N25; Secondary 11L20, 11N36.
Key words and phrases: polynomials over prime numbers, distribution in arithmetic progressions.

DOI: 10.4064/aa150-3-5

Let $R(x)$ be this number of solutions. Then we have the equality

$$R(x) = \int_0^1 \Big| \sum_{p \le x} e(\alpha p^2) \Big|^6 d\alpha. \tag{1.1}$$

As usual, we define $e(t) := \exp(2\pi i t)$. It is obvious that (1.1) is quite comfortable to be treated by the circle method, and the fact that the exponential sum appears with an exponent at least 5 is crucial when we bound the contribution of the minor arcs.

In the present paper, we choose a different quadratic form by considering

$$A(X, Y, Z) := XY + XZ + YZ.$$

Along the same lines as the above discussion, we propose

Conjecture 1.1. Every sufficienty large integer N, satisfying $N \equiv 0$ or 2 mod 3 and $N \equiv 3 \bmod 4$, can be written in the form $N = A(p_1, p_2, p_3)$.

We must explain the origin of the congruence restrictions concerning N in Conjecture 1.1. By the Chinese Remainder Theorem, we have to consider the local conditions

$$A(X, Y, Z) \equiv N \bmod p^\ell \quad \text{with } p \nmid XYZ, \tag{1.2}$$

for every $p \ge 2$ and $\ell \ge 1$.

When $p^\ell = 4$, the congruence (1.2) is solvable if and only if $N \equiv 3 \bmod 4$. Suppose that $p = 2$ and $\ell \ge 3$. If X, Y and Z are odd, then at least one of the sums $X+Y$, $X+Z$ and $Y+Z$ is not divisible by 4. Suppose that $4 \nmid X+Y$; then one has the equality $A(X, Y, Z+2^{\ell-2}) \equiv 2^{\ell-1} + A(X, Y, Z) \bmod 2^\ell$. By induction over ℓ, one deduces that (1.2) is solvable for $p = 2$ and $\ell \ge 2$ if and only if $N \equiv 3 \bmod 4$.

If $p \ge 3$ and $p \nmid XYZ$, at least one of the numbers $X+Y$, $X+Z$ and $Y+Z$ is not divisible by p. Suppose that $p \nmid X+Y$. Then for every integer k one has the equality $A(X, Y, Z+kp^\ell) \equiv A(X, Y, Z) + k(X+Y)p^\ell \bmod p^{\ell+1}$. Hence, we can lift any solution of (1.2) modulo p^ℓ to a solution modulo $p^{\ell+1}$. It remains to study (1.2) when $p \ge 5$ and $\ell = 1$. It is sufficient to remark the equalities $A(X, 1, 1) = 2X+1$ and $A(X, 2, 1) = 3X+2$ and the fact that any congruence class modulo p is of the form $2X+1$ or $3X+2$ with $p \nmid X$.

The result of Blomer and Brüdern [2] has an analogue in the context of the quadratic form A, in other words, every integer satisfying the hypotheses of Conjecture 1.1 can be written as $N = A(n_1, n_2, n_3)$ where $n_1 n_2 n_3$ has very few prime factors (see [22, p. 394] for instance). The fact that A is isotropic over $\mathbb{Q}$ simplifies the situation a lot. For the general case of an indefinite ternary anisotropic quadratic form, see [22, Corollary 2.3]. Hua's approach, based on the circle method, seems difficult to transpose to the case of the quadratic form A. Of course, Gauss reduction theory of quadratic forms,

giving here the trivial equality

$$A(X,Y,Z)=\frac{1}{4}(X+Y+2Z)^2-\frac{1}{4}(X-Y)^2-Z^2,$$

is useful after linear changes of variables when the variables X, Y and Z are given integral values, but it remains inefficient when X, Y and Z are now given prime values.

We show less pretension by studying some multiplicative properties of the values of the finite sequence (or multiset)

$$\mathcal{A}_3(x):=(p_1p_2+p_1p_3+p_2p_3)_{p_i\sim x} \tag{1.3}$$

where x is a large number and, here and throughout the paper, the notation $n\sim N$ means that n must satisfy the inequality $N<n\leq 2N$. To shorten some formulas, we also use

$$\mathcal{L}:=\log(2x),\qquad \widetilde{\pi}(x):=\pi(2x)-\pi(x),$$

where $\pi(x)$ is the usual counting function of primes $p\leq x$. We also consider the set of triples of primes $\mathcal{T}(x)=\{(p_1,p_2,p_3)\ ;\ p_1,p_2,p_3\sim x\}$. Hence, we directly have

$$\sharp\mathcal{T}(x)=\sharp\mathcal{A}_3(x)=\widetilde{\pi}(x)^3\quad(\sim x^3\mathcal{L}^{-3},\ \text{when } x\to\infty).$$

Let $n\geq 1$ be an integer. When $n\geq 2$, $P^+(n)$ is the greatest prime factor of n and we put $P^+(1)=1$. As usual, we denote by $\varphi(n)$, $\mu(n)$ and $\tau(n)$ the Euler function, the Möbius function and the number of positive divisors of n, respectively. Furthermore, $\Omega(n)$ and $\omega(n)$ indicate as usual the number of prime divisors of n, counted with and without multiplicities. We use well-known properties of these functions, which can be found, for example, in [11]. The Euler constant is denoted by γ.

As usual, $X\ll Y$ is equivalent to $X=O(Y)$ where the implied constant may occasionally, where obvious, depend on the small positive parameter ε. The dependency on some other parameters $\rho_1,\rho_2,\dots$ is indicated as $\ll_{\rho_1,\rho_2,\dots}$ or $O_{\rho_1,\rho_2,\dots}$.

1.2. Main results. Our central result gives an asymptotic formula for the number of elements—counted with multiplicity—of $\mathcal{A}_3(x)$, divisible by q, with a large uniformity over q.

THEOREM 1.2. *For every positive ε and A, the equality*

$$\begin{aligned}&\sharp\{(p_1,p_2,p_3)\in\mathcal{T}(x)\ ;\ A(p_1,p_2,p_3)\equiv 0 \bmod q\}\\&\quad=\prod_{p\mid q}\Big(1-\frac{1}{(p-1)^2}\Big)\frac{\widetilde{\pi}(x)^3}{q}+O_A\bigg(\Big(\mathcal{L}^{-A}+\mathcal{L}^5\sum_{\substack{t\mid q\\ t\geq\mathcal{L}^A}}\Big(\frac{\tau(t)}{t}\Big)^{1/2}\Big)\frac{\widetilde{\pi}(x)^3}{q}\bigg),\end{aligned}$$

holds uniformly for $x\geq 2$ and integer q satisfying $1\leq q\leq x^{17/16-\varepsilon}$.

The above result is trivial when q is even, since all the elements of $\mathcal{A}_3(x)$ are odd for $x \geq 2$. We could be more specific in the estimate of Theorem 1.2 by inserting the mutual sizes of q and x (for more precise upper bounds, see the different cases in §4.1). Let $\Xi(q, L)$ be the arithmetic factor

$$\Xi(q, L) := \sum_{\substack{t|q \\ t \geq L}} \left(\frac{\tau(t)}{t}\right)^{1/2}.$$

The factor $\Xi(q, \mathcal{L}^A)$ can be very large for special q. More precisely, by fixing $q^\dagger = 2 \cdot 3 \cdot 5 \cdot 7 \cdots$, it is standard to prove that there exists an absolute positive constant c_1 such that we have the lower bound

$$\Xi(q^\dagger, \mathcal{L}^A) \geq c_1 \exp\left(c_1 \frac{\log^{1/2} q^\dagger}{\log\log q^\dagger}\right) - \mathcal{L}^A,$$

which implies that, for any A, B and $C > 0$, the inequality

$$\max_{q \text{ odd}, \, q \sim x^C} \Xi(q, \mathcal{L}^A) \geq \mathcal{L}^B$$

is true for sufficiently large x. However, a direct computation shows that $\Xi(q, \mathcal{L}^A)$ is small most of the time, since we have

$$\sum_{q \sim Q} \Xi(q, L) \ll L^{-1/2} Q (\log(2L))^{\sqrt{2}-1} \tag{1.4}$$

uniformly for L and $Q \geq 1$. Then it is easy to deduce from (1.4) that for every $\varepsilon > 0$ and every B, we have

$$\sum_{q \leq x^{17/16-\varepsilon}} \left| \sharp\{(p_1, p_2, p_3) \in \mathcal{T}(x) \, ; \, A(p_1, p_2, p_3) \equiv 0 \bmod q\} - \prod_{p|q} \left(1 - \frac{1}{(p-1)^2}\right) \frac{\widetilde{\pi}(x)^3}{q} \right| \ll_B \widetilde{\pi}(x)^3 \mathcal{L}^{-B} \tag{1.5}$$

uniformly for $x \geq 2$. In other words, we have the expected behaviour

$$\sharp\{(p_1, p_2, p_3) \in \mathcal{T}(x) \, ; \, A(p_1, p_2, p_3) \equiv 0 \bmod q\} \sim \prod_{p|q} \left(1 - \frac{1}{(p-1)^2}\right) \frac{\widetilde{\pi}(x)^3}{q}$$

for most of the odd $q \sim Q$, with $Q \leq x^{17/16-\varepsilon}$.

Recall that the multiset $\mathcal{A}_3(x)$ contains $\widetilde{\pi}(x)^3$ elements of size at most $12x^2$. Hence, by the terminology of sieve, we say that the *exponent of distribution* of $\mathcal{A}_3(x)$ is at least $(17/16)/2 = 17/32$. This value is quite interesting since it is larger than $1/2$ and allows us to use classical sieve results in a quite efficient manner. The first example comes from the weighted sieve (for an introduction see [10, Chap. 9] or [9, Chap. 5]) and allows us to assert the existence of many elements of $\mathcal{A}_3(x)$ with very few prime factors.

COROLLARY 1.3. *There exists an absolute positive constant c_2 such that, for sufficiently large x,*

$$\sharp\{(p_1,p_2,p_3)\in\mathcal{T}(x)\,;\ \omega(A(p_1,p_2,p_3))\le 2 \\ \text{and } p\,|\,A(p_1,p_2,p_3)\Rightarrow p\ge x^{c_2}\}\ge c_2\widetilde{\pi}(x)^3\mathcal{L}^{-1}.$$

Proof. It is a direct application of the deep result of Greaves [8] so we only give brief indications on the way to apply it. Following the notation of that work, we have in our present situation

$$\begin{cases}\mathcal{A}:=\mathcal{A}_3(x),\\ X:=\widetilde{\pi}(x)^3,\\ \gamma(p):=1-(p-1)^{-2}\quad\text{for } p\ge 2,\\ y:=x^{17/16-\varepsilon},\\ g:=(\log(12x^2))/\log y\le 32/17+2\varepsilon.\end{cases}$$

Finally, by [8, equation (1.5)], we have the inequality

$$\delta_2<0.068\ldots,$$

where δ_2 is the standard constant in the theory of weighted sieve. Since $g<2-\delta_2$, we deduce Corollary 1.3 by [8, p. 298] (see also [9, Chap. 5, Proposition 1]). For better upper bounds for δ_2, see [8, p. 331] or [9, pp. 174–175].

We can even replace the function ω by Ω in the statement of Corollary 1.3 by proceeding as follows: let $\rho(n)$ be the number of solutions of the equation $n=A(p_1,p_2,p_3)$ with $p_i\sim x$. Writing this equality in the form

$$n+p_3^2=(p_1+p_3)(p_2+p_3),$$

we deduce that ρ satisfies

$$\rho(n)\le\sum_{t\sim x}\tau(n+t^2)\le 2\sum_{d\le 4x}\sum_{\substack{t\sim x\\ n+t^2\equiv 0\bmod d}}1.$$

We now insert the general inequality

$$\sharp\{t \bmod d\ ;\ t^2+n\equiv 0 \bmod d\}=O(\tau(d)(d,n)^{1/2}),$$

to deduce

$$\rho(n)\ll\sum_{d\le 4x}\tau(d)(d,n)^{1/2}\left(\frac{x}{d}+1\right)\ll x\sum_{d\le 4x}\frac{\tau(d)(d,n)^{1/2}}{d}.$$

It remains to sum over $\delta\,|\,n$ to finally prove

$$\rho(n)\ll\tau(n)x\mathcal{L}^2. \tag{1.6}$$

The inequality (1.6) allows us to consider the sum

$$\sum_{\substack{n\in\mathcal{A}_3(x)\\ \Omega(n)>\omega(n)\\ p|n\Rightarrow p>x^{c_2}}} 1 \le \sum_{p>x^{c_2}} \sum_{\substack{n\le 12x^2\\ p^2|n}} \rho(n) \ll x^{1+\varepsilon} \sum_{p>x^{c_2}} \frac{x^2}{p^2} \ll x^{3-c_2/2}.$$

This shows that the contribution of non-squarefree integers is negligible in the cardinality studied in Corollary 1.3. ∎

We note that the constant c_2 in Corollary 1.3 if effectively computable and can be made explicit.

Now we mention two consequences of a variant of (1.5) coming from the landscape of the half-dimensional sieve. This leads to the following lower bounds with a correct order of magnitude. We have:

COROLLARY 1.4. *There exists an absolute $c_3 > 0$ such that, for sufficiently large x,*

$$\sharp\{(p_1,p_2,p_3)\in\mathcal{T}(x)\ ;\ p\,|\,A(p_1,p_2,p_3)\Rightarrow p=3 \text{ or } p\equiv 1 \bmod 4\} \ge c_3\widetilde{\pi}(x)^3\mathcal{L}^{-1/2}$$

and

$$\sharp\{(p_1,p_2,p_3)\in\mathcal{T}(x)\ ;\ p\,|\,p_1p_2+p_1p_3-p_2p_3\Rightarrow p\equiv 1 \bmod 4\} \ge c_3\widetilde{\pi}(x)^3\mathcal{L}^{-1/2}.$$

Proof. For $x > 2$, any element of $n \in \mathcal{A}_3(x)$ is congruent to 3 modulo 4 so n has an odd number of prime divisors $p \equiv 3 \bmod 4$, counted with multiplicity. Consider the following subset of $\mathcal{A}_3(x)$:

$$\widetilde{\mathcal{A}}_3(x) := (A(p_1,p_2,p_3))_{\substack{p_i\sim x\\ p_i\equiv 1 \bmod 9}}.$$

For all $n \in \widetilde{\mathcal{A}}_3(x)$, we have $3 \,\|\, n$, hence each n has an even number of prime divisors (with multiplicity) larger than 3. We also have

$$\sharp\widetilde{\mathcal{A}}_3(x) \sim \frac{\widetilde{\pi}(x)^3}{216} \quad (x\to\infty),$$

as the consequence of the Prime Number Theorem for arithmetic progressions. The proofs leading to Theorem 1.2 and to (1.5) can easily be transposed to give

(1.7)
$$\sum_{\substack{q\le x^{17/16-\varepsilon}\\ 3\nmid q}} \left| \sharp\{(p_1,p_2,p_3)\in\mathcal{T}(x)\ ;\ p_i\equiv 1 \bmod 9,\ A(p_1,p_2,p_3)\equiv 0 \bmod q\} - \prod_{p|q}\left(1-\frac{1}{(p-1)^2}\right)\frac{\widetilde{\pi}(x)^3}{216\,q}\right| \ll_B \widetilde{\pi}(x)^3\mathcal{L}^{-B},$$

which is true for every $\varepsilon > 0$, and every B, uniformly for $x \ge 2$.

We sieve the multiset $\widetilde{\mathcal{A}}_3(x)$ by the set of primes

$$\mathcal{P} := \{p > 5 \ ; \ p \equiv 3 \bmod 4, \ p \le z\},$$

with $z = (12x^2)^{1/2}$. By (1.7) and by the definition of $\mathcal{P}$, the dimension κ of this sieve problem is $\kappa = 1/2$. With the notation of sieves (see [19, p. 172]), we have

$$s := \frac{\log x^{17/16-\varepsilon}}{\log z} > 1.$$

Hence, by for instance [18, Theorem 1] or [20, §9], we know that the sieving limit $\beta_{1/2}$ in dimension $1/2$ is $\beta_{1/2} = 1$. From the inequality $s > \beta_{1/2}$ we deduce that, in $\widetilde{\mathcal{A}}_3(x)$, there are at least $c_3\widetilde{\pi}(x)^3\mathcal{L}^{-1/2}$ elements with no prime divisor in $\mathcal{P}$. Then, for such elements, we easily deduce that the only prime divisor $p \equiv 3 \bmod 4$ is $p = 3$, since every element of $\widetilde{\mathcal{A}}_3(x)$ has at most one prime divisor greater than z. This yields the first part of Corollary 1.4.

For the second part of Corollary 1.4, we introduce the multiset

$$\mathcal{B}_3(x) := (p_1p_2 + p_1p_3 - p_2p_3)_{p_i \sim x},$$

and now

$$\mathcal{P} := \{p \ge 3 \ ; \ p \equiv 3 \bmod 4, \ p \le z\},$$

with the same value for z. For $x \ge 2$, all the elements of $\mathcal{B}_3(x)$ are congruent to 1 modulo 4, so they have an even number of prime divisors that are congruent to 3 modulo 4. It is now an exercise to see that Theorem 1.2 and (1.5) remain true when $\mathcal{A}_3(x)$ is replaced by $\mathcal{B}_3(x)$. By the same sifting process as for $\widetilde{\mathcal{A}}_3(x)$, we deduce that $\mathcal{B}_3(x)$ contains at least $c_3\widetilde{\pi}(x)^3\mathcal{L}^{-1/2}$ elements with no prime divisor in $\mathcal{P}$. So these elements have an even number of prime divisors that are congruent to 3 modulo 4 and $> z$. The only possibility is to have no such prime divisor; this leads to the second part of Corollary 1.4. ∎

An important ingredient in the proof of Theorem 1.2 is Lemma 2.2 below, concerning the number of solutions of Cayley's congruence modulo q, defined in (2.2) below. When averaging over q, we have a better control of this number (see Lemma 2.3). This leads to an improvement of (1.5). More precisely:

THEOREM 1.5. *For every $\varepsilon > 0$ and every B,*

$$\sum_{q \le x^{14/13-\varepsilon}} \left| \sharp\{(p_1,p_2,p_3) \in \mathcal{T}(x) \ ; \ A(p_1,p_2,p_3) \equiv 0 \bmod q\} - \prod_{p \mid q}\left(1 - \frac{1}{(p-1)^2}\right)\frac{\widetilde{\pi}(x)^3}{q}\right| \ll_B \widetilde{\pi}(x)^3\mathcal{L}^{-B}$$

uniformly for $x \ge 2$.

We now give an application of Theorem 1.5 concerning the existence in $\mathcal{A}_3(x)$ of elements with a very large prime factor. Let $\vartheta_0 = 1.10028\ldots$ be the unique root of the equation

$$13\vartheta - 16 + 12\log\left(\frac{13\vartheta - 12}{2}\right) = 0.$$

We have

COROLLARY 1.6. *For every $\vartheta < \vartheta_0$ there exist $c_4(\vartheta) > 0$ and $x_0(\vartheta)$ such that, for $x > x_0(\vartheta)$,*

$$\sharp\{(p_1, p_2, p_3) \in \mathcal{T}(x)\ ;\ P^+(A(p_1, p_2, p_3)) > x^{\vartheta}\} \geq c_4(\vartheta)\widetilde{\pi}(x)^3.$$

In particular, we can take

$$\vartheta = \frac{11}{10}.$$

Of course, Corollary 1.6 is a direct consequence of Theorem 1.5 if the constant ϑ_0 is replaced by $14/13$. We also conjecture that it holds with $\vartheta_0 = 2$. Such a conjecture is true if the quadratic form A is replaced by $X^2+Y^2+Z^2$. This is a direct consequence of Hua's result [16], since the set of integers N such that $P^+(N) > N^{1-\varepsilon}$ has a positive natural density, for every $\varepsilon > 0$. The proof of Corollary 1.6 is given in §4.3. Similarly, we could be interested in searching smooth elements in $\mathcal{A}_3(x)$.

In order to prove Theorem 1.2 we estimate exponential sums over reciprocals of primes, see §3. We denote by $\overline{n} \bmod q$, or $\overline{n}$ when the context is obvious, for instance in the fraction $\overline{n}/q$, the multiplicative inverse of n modulo q when $(n, q) = 1$.

2. Preparatory results

2.1. Kloosterman sums. First recall the classical upper bound for short Kloosterman–Ramanujan sums (for a weaker result see [15, Lemma 4, p. 36]).

LEMMA 2.1. *One has the inequality*

$$\sum_{\substack{Y < n \leq Z \\ (n,q)=1}} e\left(a\frac{\overline{n}}{q}\right) \ll \left(\mu\left(\frac{q}{(a,q)}\right)\right)^2 \left(\frac{Z-Y}{q} + 1\right) \cdot \frac{\varphi(q)}{\varphi\left(\frac{q}{(a,q)}\right)} + \tau(q)\tau((a,q))(\log(2q))q^{1/2},$$

for all integers a and q with $q \geq 1$ and $Y < Z$.

Proof. First split the interval of summation into consecutive intervals of length equal to q. Their number is $O((Z-Y)/q)$. On each of these subin-

tervals, the value of the exponential sum is the well-known Ramanujan sum

$$\sum_{\substack{n=1\\(n,q)=1}}^{q} e\Big(a\frac{n}{q}\Big) = \mu\Big(\frac{q}{(a,q)}\Big)\cdot\frac{\varphi(q)}{\varphi\big(\frac{q}{(a,q)}\big)},$$

by [11, Theorem 272]. By a classical method we develop in Fourier series the characteristic function of the remaining interval $\mathcal{I}$, leading to the equality

$$\begin{aligned}\sum_{\substack{n\in\mathcal{I}\\(n,q)=1}} e\Big(a\frac{\overline{n}}{q}\Big) &= \frac{1}{q}\sum_{\ell=0}^{q-1}\sum_{m\in\mathcal{I}}\sum_{\substack{n=0\\(n,q)=1}}^{q-1} e\Big(\ell\frac{m-n}{q}\Big)e\Big(a\frac{\overline{n}}{q}\Big)\\ &= \frac{1}{q}\sum_{\ell=0}^{q-1}\Big(\sum_{m\in\mathcal{I}} e\Big(\frac{\ell m}{q}\Big)\Big)\mathrm{Kl}(-\ell,a;q),\end{aligned}\tag{2.1}$$

where $\mathrm{Kl}(a,b;q)$ is the Kloosterman sum

$$\mathrm{Kl}(a,b;q) := \sum_{\substack{n=0\\(n,q)=1}}^{q-1} e\Big(\frac{an+b\overline{n}}{q}\Big).$$

In (2.1), we separate the case $\ell=0$ from the other ℓ, use symmetry $\ell\mapsto q-\ell$ and appeal to the well-known bound

$$\mathrm{Kl}(a,b;q) \ll (a,b,q)^{1/2}\tau(q)q^{1/2}$$

to finally write the inequality

$$\sum_{\substack{n\in\mathcal{I}\\(n,q)=1}} e\Big(a\frac{\overline{n}}{q}\Big) \ll \Big(\mu\Big(\frac{q}{(a,q)}\Big)\Big)^2\cdot\frac{\varphi(q)}{\varphi\big(\frac{q}{(a,q)}\big)} + \tau(q)q^{1/2}\sum_{\ell=1}^{\lfloor q/2\rfloor}\frac{(a,\ell,q)^{1/2}}{\ell}.$$

Summing over the divisors of (a,q), we obtain

$$\sum_{\substack{n\in\mathcal{I}\\(n,q)=1}} e\Big(a\frac{\overline{n}}{q}\Big) \ll \Big(\mu\Big(\frac{q}{(a,q)}\Big)\Big)^2\cdot\frac{\varphi(q)}{\varphi\big(\frac{q}{(a,q)}\big)} + \tau((a,q))\tau(q)q^{1/2}\log(2q),$$

which concludes the proof. ∎

2.2. Cayley's congruence. An important tool of our proofs will be considerations of Cayley's congruence

$$\overline{n_1}+\overline{n_2}\equiv\overline{n_3}+\overline{n_4} \bmod q,\tag{2.2}$$

where the unknowns are the integers n_i and $(n_i,q)=1$. For $K\geq 1$, we denote by $J_K(q)$ the number of solutions of (2.2) with the extra condition $1\leq n_i\leq K$.

LEMMA 2.2. *For every $\varepsilon > 0$, we have*

$$J_K(q) \ll (K^{7/2}q^{-1/2} + K^2)q^{\varepsilon}$$

for all $q \geq 1$ and K satisfying $1 \leq K \leq q$.

Proof. This is an extension of [7, Lemma 2.3]. Turning to the original proof of Heath-Brown ([13, pp. 367–368]), we define $m(s)$ as the number of solutions of the congruence $\overline{n_1} + \overline{n_2} \equiv s \bmod q$, with the constraint $1 \leq n_i \leq K$ and $(n_i, q) = 1$. We trivially have

$$J_K(q) = \sum_{s=0}^{q-1} m(s)^2.$$

Discussing the respective sizes of (s, q) and q/K, we can prove the inequality

$$\sum_{s=0}^{q-1} m(s)^2 \ll (K^{7/2}q^{-1/2} + K^2)q^{\varepsilon}$$

(see [13, p. 368]). This concludes the proof. ∎

LEMMA 2.3. *For every $\varepsilon > 0$, we have*

$$\sum_{q \sim Q} J_K(q) \ll (K^2Q + K^4)K^{\varepsilon}$$

for all K and $Q \geq 1$.

Proof. Let $\boldsymbol{n} = (n_1, n_2, n_3, n_4)$ and $P(\boldsymbol{n}) = n_1n_3n_4 + n_2n_3n_4 - n_1n_2n_3 - n_1n_2n_4$. Multiplying by $n_1n_2n_3n_4$ and inverting the summations, we trivially have

$$\begin{aligned}\sum_{q \sim Q} J_K(q) &\ll Q \sharp\{\boldsymbol{n} \,;\, n_i \leq K,\, P(\boldsymbol{n}) = 0\} + \sum_{\substack{\boldsymbol{n},\, n_i \leq K \\ P(\boldsymbol{n}) \neq 0}} \tau(P(\boldsymbol{n})) \\ &\ll (K^2Q + K^4)K^{\varepsilon},\end{aligned}$$

by appealing, for instance, to the result of Heath-Brown [14, Theorem, p. 2] on the number of non-trivial integer points of height at most K on Cayley's cubic surface defined by $P(\boldsymbol{X}) = 0$, where $\boldsymbol{X} = (X_1, X_2, X_3, X_4)$. ∎

2.3. Double exponential sums. The following estimate is an extension of a result of Garaev [7, Lemma 2.4]. For its statement, we consider the general double sum

$$\mathfrak{S}(a, q, \boldsymbol{\beta}, L, M, (M_\ell)) := \sum_{\substack{\ell=1 \\ (\ell,q)=1}}^{L} \Bigg| \sum_{\substack{m=1 \\ (m,q)=1}}^{M_\ell} \beta_m e\bigg(a\frac{\overline{\ell}\,\overline{m}}{q}\bigg)\Bigg|,$$

where

(i) a and q are coprime integers with $q \geq 1$,
(ii) L and M are positive integers,

(iii) $(M_\ell)_{1\le\ell\le L}$ is a sequence of numbers satisfying $1 \le M_\ell \le M$,
(iv) $\boldsymbol{\beta} = (\beta_m)_{m\le M}$ is a finite sequence of complex numbers of ℓ_∞-norm $\|\boldsymbol{\beta}\|_\infty$.

We now state an estimate of $\mathfrak{S}$ in terms of $J_K(q)$ which is essentially contained in the proof of [7, Lemma 2.4]; see also [21, Lemma 4] (the fact that the modulus is prime in [7, 21] plays no role in the argument).

LEMMA 2.4. *For every positive ε, for every choice of the parameters as in* (i)–(iv) *above, with the extra condition*

$$L, M \le q,$$

the following holds:

(2.3)
$$\mathfrak{S}(a,q,\boldsymbol{\beta},L,M,(M_\ell)) \ll \|\boldsymbol{\beta}\|_\infty q^\varepsilon \min\{q^{1/8}L^{1/2}M^{1/2}J_L(q)^{1/8}J_M(q)^{1/8}, q^{1/4}L^{3/4}J_M(q)^{1/4}, q^{1/4}M^{3/4}J_L(q)^{1/4}\}.$$

The general upper bound of Lemma 2.4 is adapted to the application of Lemma 2.3 when we sum over q. Individually, for every q, using Lemma 2.2 instead of [7, Lemma 2.3] we obtain a full analogue of [7, Lemma 2.4]:

COROLLARY 2.5. *For every positive ε, and every choice of the parameters as in* (i)–(iv) *above with the extra condition*

$$L, M \le q,$$

the following hold:

(a) *if $q^{1/3} \le L, M \le q$, we have*
$$\mathfrak{S}(a,q,\boldsymbol{\beta},L,M,(M_\ell)) \ll \|\boldsymbol{\beta}\|_\infty q^\varepsilon L^{15/16}M^{15/16},$$
(b) *if $L \le q^{1/3}$ and $M \le q$, we have*
$$\mathfrak{S}(a,q,\boldsymbol{\beta},L,M,(M_\ell)) \ll \|\boldsymbol{\beta}\|_\infty q^{1/4+\varepsilon}L^{1/2}M^{3/4},$$
(c) *if $M \le q^{1/3}$ and $L \le q$, we have*
$$\mathfrak{S}(a,q,\boldsymbol{\beta},L,M,(M_\ell)) \ll \|\boldsymbol{\beta}\|_\infty q^{1/4+\varepsilon}L^{3/4}M^{1/2}.$$

Similarly, using Lemma 2.3 instead of Lemma 2.2 (and using only the last estimate of Lemma 2.4), together with the bound

$$\sum_{q\sim Q} J_K(q)^{1/4} \le Q^{3/4}\Big(\sum_{q\sim Q} J_K(q)\Big)^{1/4}$$

implied by the Hölder inequality, we obtain:

COROLLARY 2.6. *For every positive ε, and every choice of the parameters as in* (i)–(iv) *above with the extra condition*

$$L, M \le Q,$$

we have

$$\sum_{q\sim Q}\max_{(a,q)=1}\mathfrak{S}(a,q,\boldsymbol{\beta},L,M,(M_\ell))\ll\|\boldsymbol{\beta}\|_\infty Q^\varepsilon(Q^{5/4}L^{1/2}M^{3/4}+QLM^{3/4}).$$

We note that we formulated Corollary 2.6 in a convenient way for our applications; using the full power of Lemma 2.4 one gets a series of other estimates.

Finally, the bounds of Corollaries 2.5 and 2.6 are complemented by the following estimate which is derived directly from Lemma 2.1. In the case of prime q this bound is given in the final part of the proof of [7, p. 372] and the proof easily extends to arbitrary integers $q\ge 2$; in fact an almost identical sum is also estimated in [6, §2] (for arbitrary composite q); see also our estimate of the sums $W_4(M,N)$ in §3.3.

LEMMA 2.7. *For every positive ε, and every choice of the parameters as in* (i)–(iv) *above with the extra condition*

$$L,M\le q,$$

we have

$$\mathfrak{S}(a,q,\boldsymbol{\beta},L,M,(M_\ell))\ll\|\boldsymbol{\beta}\|_\infty q^\varepsilon(LM^{1/2}+q^{1/4}L^{1/2}M).$$

3. The central exponential sum

3.1. Notation and background. This section is devoted to the study of the exponential sum

$$S_q(a;x):=\sum_{\substack{x<p\le 2x\\(p,q)=1}}e\Big(a\frac{\overline{p}}{q}\Big),$$

where $x\ge 2$ is a real number, $q\ge 2$ is an integer, not necessarily prime. We have in mind to treat $S_q(a;x)$ when q and x have comparable orders of magnitude, with some emphasis on the case $x\le q$. Note that we may change the conditions of summations into $2\le p\le x$, $(p,q)=1$, without any effort, the upper bounds are the same, up to a constant factor.

As far as we know, this problem has a rather short history. Using bounds for multidimensional exponential sums coming from algebraic geometry, Fouvry and Michel [5, Théorème 1.1] have proved the general upper bound

$$\sum_{\substack{x<p\le 2x\\(p,q)=1}}e\Big(\frac{f(p)}{q}\Big)\ll_f q^{3/16+\varepsilon}x^{25/32}$$

for every $\varepsilon>0$, q prime, $2\le x\le q$, and $f(X)$ a rational function with integer coefficients, different from a polynomial of $\mathbb{Z}[X]$ with degree 0 or 1. Their general method could be even specialized to the case where $f(X)$ is

a quasi-monomial (which means $f(X) = X^k + ux$, with $k \in \mathbb{Z} \setminus \{0, 1\}$ and $u \in \mathbb{Z}$). In particular, they proved that, for every $\delta > 0$, there exists a positive η such that

$$S_q(a; x) \ll_\delta x^{1-\eta} \tag{3.1}$$

uniformly for q prime, $(a, q) = 1$ and $q^{3/4+\delta} \le x \le q$ (see [5, Corollaire 1.6]).

By sum-product techniques, Bourgain [3, Theorem A.9] proved that (3.1) is in fact true when $q^{1/2+\delta} \le x \le q$.

Then Garaev [7, Theorem 1.1] proved that

$$S_q(a; x) \ll (x^{15/16} + q^{1/4}x^{2/3})q^\varepsilon, \tag{3.2}$$

for every $\varepsilon > 0$, uniformly for q prime, $(a, q) = 1$ and $2 \le x \le q$. The upper bound (3.2) is valuable in the interval $q^{3/4+\varepsilon} \le x \le q$ and it can be interpreted as an effective version of (3.1), but the methods are quite different: Garaev incorporates results, due to Heath-Brown, concerning Cayley's congruence $\overline{n_1} + \overline{n_2} - \overline{n_3} - \overline{n_4} \equiv 0 \bmod p$ in small boxes (see Lemma 2.2 above), and only uses Weil's bound for Kloosterman sums via Karatsuba's method.

3.2. Large denominators. We extend Garaev's work [7] to composite moduli and x larger than q by the following

THEOREM 3.1. *For every $\varepsilon > 0$,*

$$S_q(a; x) \ll (x^{15/16} + q^{1/4}x^{2/3})q^\varepsilon$$

uniformly for $q \ge 2$, $(a, q) = 1$, and $x \ge 2$ satisfying $x^{3/4} \le q \le x^{4/3}$.

Proof. It is a paraphrase of Garaev's proof [7], so we only indicate the modifications of his original proof to obtain this generalization. It is based on the results contained in §2 and on Vaughan's identity (see [4, Chap. 24]) to enter in the combinatorial structure of the characteristic function of primes, or equivalently, of the von Mangoldt function Λ, which we recall to be defined for positive integers n by

$$\Lambda(n) = \begin{cases} \log p & \text{if } n > 1 \text{ is a power of a prime } p, \\ 0 & \text{otherwise.} \end{cases}$$

As usual, it is sufficient to prove the same inequality—up to a log factor—for the sum $\widetilde{S}_q(a; x)$, where

$$\widetilde{S}_q(a; x) := \sum_{n \le x} \Lambda(n) e\left(a\frac{\overline{n}}{q}\right).$$

When x satisfies the inequality $q^{3/4} \le x \le q$, the proof is the same as in [7, §3], if we replace [7, Lemma 2.4] by its extension to the case of q composite, as in Corollary 2.5, and if we use Lemma 2.7 instead of the similar estimate in [7] obtained only for prime q.

Hence there remains the case

$$q \le x \le q^{4/3}. \tag{3.3}$$

One more time, we exploit [7, §3] to shorten the proof. Fix

$$U = V = q^{1/3}.$$

By the Vaughan identity (see [4, Chap. 24]), we have

$$|\widetilde{S}_q(a;x)| \le W_1 + W_2 + W_3 + W_4, \tag{3.4}$$

where

$$W_1 := \left|\sum_{n\le U} \Lambda(n) e\left(a\frac{\overline{n}}{q}\right)\right|, \qquad W_2 := \sum_{n\le UV} (\log n)\left|\sum_{m\le x/n} e\left(a\frac{\overline{m}\,\overline{n}}{q}\right)\right|,$$

$$W_3 := \sum_{n\le V}\left|\sum_{m\le x/n} (\log m) e\left(a\frac{\overline{m}\,\overline{n}}{q}\right)\right|, \quad W_4 := \sum_{U<n\le x/V} \Lambda(n)\left|\sum_{V<m\le x/n} \beta_m e\left(a\frac{\overline{m}\,\overline{n}}{q}\right)\right|.$$

In all these expressions the variables of summation m and n are coprime with q, and β_m is some arithmetic coefficient which satisfies

$$|\beta_m| \le \tau(m) \quad (m \ge 1).$$

Hence the proof is complete as soon as we have proved

$$W_i \ll (x^{15/16} + q^{1/4}x^{2/3})x^{\varepsilon} \quad (i = 1,2,3,4), \tag{3.5}$$

under the condition (3.3).

We trivially have $W_1 \ll q^{1/3}$, hence (3.5) is satisfied.

To treat W_2, we first cover the range of summation $[1, UV]$ with $O(\mathcal{L})$ dyadic intervals $L < n \le 2L$. We call $W_2(L)$ the corresponding subsum and consider two cases.

- If $L \le q^{1/3}$, the variable m has a long range of variation. Hence it is worth to apply Lemma 2.1 to deduce that the corresponding subsum satisfies

$$\begin{aligned} W_2(L) &\ll \mathcal{L}\sum_{n\sim L}\left\{\mu(q)^2\left(\frac{x}{nq}+1\right) + \tau(q)\log(2q)q^{1/2}\right\} \\ &\ll x^{\varepsilon}(q^{1/2}L + q^{-1}x) \ll q^{5/6}x^{\varepsilon} \ll x^{15/16+\varepsilon}. \end{aligned}$$

- When $q^{1/3} < L \le q^{2/3}$, the inequalities $n \sim L$ and (3.3) imply $x/n < xq^{-1/3} \le q$. Then Corollary 2.5(a) is applicable to $W_2(L)$, giving the same upper bound

$$W_2(L) \ll q^{\varepsilon}L^{15/16}(x/L)^{15/16} \ll x^{15/16+\varepsilon}. \tag{3.6}$$

It remains to sum over all the dyadic intervals and to combine the two subcases ($L < q^{1/3}$ and $q^{1/3} < L \le q^{2/3}$) to deduce that W_2 satisfies (3.5).

For W_3, we use the same technique as for W_2, subcase $L < q^{1/3}$, combined with a partial summation to take care of the $\log m$ factors. We directly deduce that (3.5) is also satisfied for W_3.

For W_4, we split the interval of summation $[U, x/V]$ into $O(\mathcal{L})$ dyadic subintervals $L < n \le 2L$. Let $W_4(L)$ be the corresponding subsum. By (3.3), we always have $q^{1/3} \le L \le q$ and $q^{1/3} \le x/n \le q$ in the conditions of summation defining $W_4(L)$. Corollary 2.5(a) implies that $W_4(L)$ satisfies (3.6). Summing over L, we deduce that (3.5) is also satisfied by W_4.

This completes the proof of Theorem 3.1. ∎

3.3. Medium denominators. In this section, we want to give an upper bound of $S_q(a;x)$ but when q satisfies the inequality

$$\mathcal{L}^7 \le q \le x^{4/5-\varepsilon}.$$

The proof is easier than the proof of Theorem 3.1, since it only requires Lemma 2.1. We have

THEOREM 3.2. *The bound*

$$S_q(a;x) \ll \tau(q)^{1/2} q^{-1/2} x \mathcal{L}^2 + \tau(q) q^{1/4} x^{4/5} \mathcal{L}^{3/2}$$

holds uniformly for $q \ge 1$, $(a,q) = 1$, *and* $x \ge 1$.

Proof. As in the proof of Theorem 3.1 in §3.2 we rather study $\widetilde{S}_q(a;x)$ and start from the decomposition (3.4). The parameters U and V are now defined by

$$U = V = x^{2/5}.$$

We trivially have

$$W_1 \ll x^{2/5}. \tag{3.7}$$

For W_4, we first split this sum into $O(\mathcal{L}^2)$ subsums, where the variables of summation satisfy $m \sim M$ and $n \sim N$, with $M, N > U = V$, $MN < x$. Let $W_4(M,N)$ be such a subsum. By the Cauchy–Schwarz inequality, we have

$$W_4^2(M,N) \ll \Big\{ \sum_{n\sim N} \Lambda(n) \Big| \sum_{\substack{m\sim M \\ mn\le x}} \beta_m e\Big(a\frac{\overline{m}\,\overline{n}}{q}\Big) \Big| \Big\}^2$$

$$\ll N\mathcal{L} \sum_{m_1,m_2\sim M} \tau(m_1)\tau(m_2) \Big| \sum_{n\le \min\{x/m_1, x/m_2\}} e\Big(a\frac{(\overline{m_1}-\overline{m_2})\overline{n}}{q}\Big) \Big|$$

$$\ll N\mathcal{L}\Bigg\{N\sum_{m\sim M}\tau(m)^2+\sum_{\substack{m_1,m_2\sim M\\ m_1\neq m_2}}\tau(m_1)\tau(m_2)$$
$$\times\left(\left(\frac{N}{q}+1\right)\frac{\varphi(q)}{\varphi\big(\frac{q}{(m_1-m_2,q)}\big)}+\tau(q)\tau((m_1-m_2,q))q^{1/2}\mathcal{L}\right)\Bigg\},$$

by Lemma 2.1. Using the inequalities $\varphi(q)/\varphi(t)\le q/t$ for all $t\,|\,q$ and $\tau(m_1)\tau(m_2)\ll\tau(m_1)^2+\tau(m_2)^2$ we simplify the above inequality to

$$W_4^2(M,N)\ll N\mathcal{L}\Bigg\{N\sum_{m\sim M}\tau(m)^2$$
$$+\sum_{\substack{m_1,m_2\sim M\\ m_1\neq m_2}}\tau(m_1)^2\left(\left(\frac{N}{q}+1\right)(m_1-m_2,q)+\tau(q)^2q^{1/2}\mathcal{L}\right)\Bigg\}.$$

By summing over $\delta=(m_1-m_2,q)$ and by using $\sum_{m\sim M}\tau(m)^2\ll M\mathcal{L}^3$ we finally get

$$W_4^2(M,N)\ll N\mathcal{L}\left\{MN\mathcal{L}^3+\tau(q)M^2\mathcal{L}^3\left(\frac{N}{q}+1\right)+\tau(q)^2q^{1/2}M^2\mathcal{L}^4\right\}$$
$$\ll MN^2\mathcal{L}^4+\tau(q)q^{-1}M^2N^2\mathcal{L}^4+\tau(q)^2q^{1/2}M^2N\mathcal{L}^5.$$

Then summing over all the $N\le xM^{-1}$ and $U<M<xU^{-1}$ (recall that M and N are in geometric progressions) we finally obtain

$$W_4\ll xU^{-1/2}\mathcal{L}^2+\tau(q)^{1/2}q^{-1/2}x\mathcal{L}^3+\tau(q)q^{1/4}xU^{-1/2}\mathcal{L}^{5/2},$$

which simplifies to

$$W_4\ll\tau(q)^{1/2}q^{-1/2}x\mathcal{L}^3+\tau(q)q^{1/4}xU^{-1/2}\mathcal{L}^{5/2}. \tag{3.8}$$

For W_2 we treat separately two subcases corresponding to the contribution of small or large values of n.

- By Lemma 2.1 we see that the subsum of W_2 corresponding to $n\le U$ is

$$W_2\ll\mathcal{L}\sum_{n\le U}\left(\frac{x}{nq}+\tau(q)q^{1/2}\mathcal{L}\right)\ll q^{-1}x\mathcal{L}^2+\tau(q)q^{1/2}U\mathcal{L}^2. \tag{3.9}$$

- For the contribution of the remaining n (with $U\le n\le U^2$) we follow the same technique as for W_4 above, leading to the same inequality as (3.8).

The treatment of W_3 is the same as of the first subsum of W_2 but with an extra partial summation to eliminate the log factor. Hence we have

$$W_3\ll q^{-1}x\mathcal{L}^3+\tau(q)q^{1/2}U\mathcal{L}^3. \tag{3.10}$$

Gathering (3.7)–(3.10) in (3.4), we obtain the inequality

$$\begin{aligned}\widetilde{S}_q(a;x) &\ll \tau(q)^{1/2}q^{-1/2}x\mathcal{L}^3 + \tau(q)q^{1/4}xU^{-1/2}\mathcal{L}^{5/2} + \tau(q)q^{1/2}U\mathcal{L}^3\\ &\ll \tau(q)^{1/2}q^{-1/2}x\mathcal{L}^3 + \tau(q)q^{1/4}x^{4/5}\mathcal{L}^{5/2},\end{aligned}$$

by the definition of U and the fact that we can suppose that $q \le x^{4/5}$, otherwise Theorem 3.2 is trivial.

By classical techniques of analytic number theory, we pass from this inequality to an inequality concerning $S_q(a;x)$ itself. ∎

3.4. Tiny denominators. In this section, we finish the study of $S_q(a;x)$ in the particular case where q is tiny, which means

$$q \le \mathcal{L}^A, \tag{3.11}$$

where A is any fixed constant. Our main ingredient is the Siegel–Walfisz Theorem that we use in the form

$$\sharp\{p \sim x\,;\ p \equiv b \bmod q\} = \frac{\widetilde{\pi}(x)}{\varphi(q)} + O_B(x\mathcal{L}^{-B}), \tag{3.12}$$

for every $B > 0$ and every b coprime with q (see [4, p. 133], for instance). By trivial transformations we see that (3.12) implies

$$\begin{aligned}S_q(a;x) &= \sum_{(b,q)=1} e\left(a\frac{\overline{b}}{q}\right)\left(\frac{\widetilde{\pi}(x)}{\varphi(q)} + O(x\mathcal{L}^{-B})\right)\\ &= \frac{\mu(q)}{\varphi(q)}\widetilde{\pi}(x) + O(\varphi(q)x\mathcal{L}^{-B}).\end{aligned} \tag{3.13}$$

This asymptotic formula is similar to the case of the sum $\sum_{p\sim x} e(ap/q)$ which appears in the major arcs in the proof of Vinogradov's Three Primes Theorem by the circle method.

3.5. Bounds on average. In this section we want to improve the upper bound given in Theorem 3.1 on average over q, by replacing Corollary 2.5 by Corollary 2.6.

THEOREM 3.3. *For every $\varepsilon > 0$,*

$$\sum_{q\sim Q}\max_{(a,q)=1}|S_q(a;x)| \ll (Q^{13/10}x^{3/5} + Q^{13/12}x^{5/6})Q^{\varepsilon}$$

uniformly for $Q^{3/2} \ge x \ge 1$.

Proof. Clearly we can assume that $x \ge Q^{3/4}$, otherwise the bound is trivial.

We follow the steps of the proof of Theorem 3.1 in §3.2. In particular, we note that it is enough to estimate

$$\Sigma := \sum_{q\sim Q} \max_{(a,q)=1} |\widetilde{S}_q(a;x)|.$$

Fix

$$U = Q^{1/2} \quad \text{and} \quad V = x^{1/2}Q^{-1/4}$$

and note that

$$UV = x^{1/2}Q^{1/4} \le \min\{Q, x\}.$$

Summing the inequality (3.4) over $q \sim Q$, we get

$$\Sigma \le \mathfrak{W}_1 + \mathfrak{W}_2 + \mathfrak{W}_3 + \mathfrak{W}_4,$$

where

$$\mathfrak{W}_1 := \sum_{q\sim Q} \max_{(a,q)=1} \left| \sum_{n\le U} \Lambda(n) e\left(a\frac{\overline{n}}{q}\right)\right|,$$

$$\mathfrak{W}_2 := \sum_{q\sim Q} \max_{(a,q)=1} \sum_{n\le UV} (\log n) \left| \sum_{m\le x/n} e\left(a\frac{\overline{m}\,\overline{n}}{q}\right)\right|,$$

$$\mathfrak{W}_3 := \sum_{q\sim Q} \max_{(a,q)=1} \sum_{n\le V} \left| \sum_{m\le x/n} (\log m) e\left(a\frac{\overline{m}\,\overline{n}}{q}\right)\right|,$$

$$\mathfrak{W}_4 := \sum_{q\sim Q} \max_{(a,q)=1} \sum_{U<n\le x/V} \Lambda(n) \left| \sum_{V<m\le x/n} \beta_m e\left(a\frac{\overline{m}\,\overline{n}}{q}\right)\right|.$$

In these expressions the variables of summation m and n are coprime with q, and β_m is some arithmetic coefficient which satisfies

$$|\beta_m| \le \tau(m) \quad (m \ge 1).$$

Hence it is enough to prove the bounds

$$\mathfrak{W}_i \ll (Q^{13/10}x^{3/5} + Q^{13/12}x^{5/6})Q^{\varepsilon} \quad (i = 1, 2, 3, 4), \tag{3.14}$$

under the conditions of Theorem 3.3.

We trivially have $\mathfrak{W}_1 \le Q^{3/2}$, hence (3.14) is satisfied.

To treat $\mathfrak{W}_2$, we first decompose the range of summation $[1, UV]$ into $O(\mathcal{L})$ dyadic intervals $L < n \le 2L$. We call $\mathfrak{W}_2(L)$ the corresponding subsum and consider the following three cases:

- If $L \le Q^{-1/5}x^{3/5}$ we apply Lemma 2.1 and, as before, we deduce that the corresponding subsum satisfies

$$\mathfrak{W}_2(L) \ll x^{\varepsilon}(Q^{3/2}L + x) \ll x^{\varepsilon}(Q^{13/10}x^{3/5} + x) \ll Q^{13/10}x^{3/5+\varepsilon}.$$

- When $Q^{-1/5}x^{3/5} < L \le Q^{1/3}x^{1/3}$, since $x \le Q^{3/2}$, the inequalities $n \sim L$ imply $x/n < Q^{1/5}x^{2/5} \le Q$. Therefore Corollary 2.6 is applicable to $\mathfrak{W}_2(L)$, giving the upper bound

$$\begin{aligned}(3.15)\qquad \mathfrak{W}_2(L) &\ll Q^{\varepsilon}(Q^{5/4}L^{1/2}(x/L)^{3/4} + QL(x/L)^{3/4})\\ &= Q^{\varepsilon}(Q^{5/4}L^{-1/4}x^{3/4} + QL^{1/4}x^{3/4})\\ &\ll Q^{\varepsilon}(Q^{5/4}(Q^{-1/5}x^{3/5})^{-1/4}x^{3/4} + Q(Q^{1/3}x^{1/3})^{1/4}x^{3/4})\\ &= Q^{\varepsilon}(Q^{13/10}x^{3/5} + Q^{13/12}x^{5/6}).\end{aligned}$$

- When $Q^{1/3}x^{1/3} < L \le UV$ we use Lemma 2.7 (for every $q \sim Q$), getting

$$\begin{aligned}(3.16)\qquad \mathfrak{W}_2(L) &\ll Q^{1+\varepsilon}(L(x/L)^{1/2} + Q^{1/4}L^{1/2}(x/L))\\ &= Q^{1+\varepsilon}(L^{1/2}x^{1/2} + Q^{1/4}L^{-1/2}x)\\ &\le Q^{1+\varepsilon}((UV)^{1/2}x^{1/2} + Q^{1/4}(Q^{1/3}x^{1/3})^{-1/2}x)\\ &= Q^{\varepsilon}(Q^{9/8}x^{3/4} + Q^{13/12}x^{5/6}) \ll Q^{13/12+\varepsilon}x^{5/6},\end{aligned}$$

since $Q^{13/12}x^{5/6} \ge Q^{9/8}x^{3/4}$ for $x \ge Q^{1/2}$.

Thus in all ranges of L the sums $\mathfrak{W}_2(L)$ are bounded by the expression on the right hand side of (3.14). It remains to sum over all the dyadic intervals to deduce that $\mathfrak{W}_2$ satisfies (3.14).

For $\mathfrak{W}_3$, we use the same technique as for $\mathfrak{W}_2$, combined with a partial summation to get rid of the $\log m$ factor. We directly see that (3.14) is also satisfied for $\mathfrak{W}_3$.

For $\mathfrak{W}_4$, we split the interval of summation $[U, x/V]$ into $O(\mathcal{L})$ dyadic subintervals $L < n \le 2L$. Let $\mathfrak{W}_4(L)$ be the corresponding subsum.

- When $U < L \le Q^{1/3}x^{1/3}$, since $x \le Q^{3/2}$, the inequalities $n \sim L$ imply $x/n < x/U = xQ^{-1/2} \le Q$. Thus using Corollary 2.6, similarly to (3.15), we derive

$$\begin{aligned}\mathfrak{W}_4(L) &\ll (Q^{5/4}U^{-1/4}x^{3/4} + Q(Q^{1/3}x^{1/3})^{1/4}x^{3/4})\\ &= Q^{\varepsilon}(Q^{9/8}x^{3/4} + Q^{13/12}x^{5/6}) \ll Q^{13/12+\varepsilon}x^{5/6},\end{aligned}$$

since $Q^{9/8}x^{3/4} \le Q^{13/12}x^{5/6}$ for $x \ge Q^{1/2}$.

- When $Q^{1/3}x^{1/3} < L \le x/V$, we use Lemma 2.7 and, quite similarly to (3.16), we derive

$$\begin{aligned}\mathfrak{W}_4(L) &\ll Q^{1+\varepsilon}((x/V)^{1/2}x^{1/2} + Q^{1/4}(Q^{1/3}x^{1/3})^{-1/2}x)\\ &\ll Q^{\varepsilon}(Q^{9/8}x^{3/4} + Q^{13/12}x^{5/6}) \ll Q^{13/12+\varepsilon}x^{5/6}.\end{aligned}$$

Again we see that in all ranges of L the sums $\mathfrak{W}_4(L)$ are bounded by the expression on the right hand side of (3.14) and summing over all the dyadic intervals we deduce that $\mathfrak{W}_4$ satisfies (3.14).

This completes the proof of Theorem 3.3. ∎

For real positive η and x, we say that q is (η, x)-*good* if for all divisors $t \mid q$ with $t \geq x$ we have

$$\max_{(b,t)=1} |S_t(b;x)| \leq (t^{3/10}x^{3/5} + t^{1/12}x^{5/6})t^{\eta}. \tag{3.17}$$

Otherwise we say that q is (η, x)-*bad*.

COROLLARY 3.4. *For every positive constant η,*

$$\sharp\{q \sim Q \ ; \ q \text{ is } (\eta, x)\text{-bad}\} \ll_{\eta} Qx^{-\eta/2}$$

uniformly for $Q \leq x^2$.

Proof. Of course, Corollary 3.4 is trivial for $Q < x/2$, since every $t \mid q$ ($\sim Q$) is less than x. By Theorem 3.3 (taken with $\varepsilon = \eta/3$) we see that for any $x/2 \leq T \leq Q$ there are at most $O_{\eta}(T^{1-2\eta/3})$ values of $t \sim T$ for which (3.17) does not hold. Now for each $t \sim T$ there are $O(Q/T)$ integers $q \sim Q$ with $t \mid q$. So there are at most $O(Qx^{-2\eta/3})$ values of $q \sim Q$ for which (3.17) fails for some divisor $t \sim T$. Covering the range $x \leq t \leq x^2$ by $O(\mathcal{L})$ dyadic intervals, we obtain the result. ∎

4. Proofs of main results

4.1. Proof of Theorem 1.2. It is a game with exponential sums and the various estimations of $S_q(a;x)$ given in the previous sections. Let

$$A(x;q) := \sharp\{(p_1,p_2,p_3) \in \mathcal{T}(x) \ ; \ p_1p_2 + p_2p_3 + p_1p_3 \equiv 0 \bmod q\} \tag{4.1}$$

be the cardinality occurring in Theorem 1.2, and

$$A^*(x;q) := \sharp\{(p_1,p_2,p_3) \in \mathcal{T}(x) \ ; \ (p_i,q) = 1, \ p_1p_2 + p_2p_3 + p_1p_3 \equiv 0 \bmod q\}$$

be the reduced cardinality. We trivially have

$$0 \leq A(x;q) - A^*(x;q) \leq 3\omega(q)\widetilde{\pi}(x). \tag{4.2}$$

Dividing by $p_1p_2p_3$, we get

$$A^*(x;q) = \sharp\{(p_1,p_2,p_3) \in \mathcal{T}(x) \ ; \ (p_i,q) = 1, \ \overline{p_1} + \overline{p_2} + \overline{p_3} \equiv 0 \bmod q\}.$$

Expressing $A^*(x;q)$ via exponential sums leads to

$$A^*(x;q) = \frac{1}{q}\sum_{a=1}^{q} S_q(a;x)^3. \tag{4.3}$$

In such an expression, the integers a and q are not necessarily coprime. Let $a/q = b/t$ where b and t are coprime. We then have

$$S_q(a;x) = S_t(b;x) + O(\mathcal{L}),$$

the error term coming from the p dividing q but not t. Taking the cube yields

$$S_q(a;x)^3 = S_t(b;x)^3 + O(\mathcal{L}|S_t(b;x)|^2 + \mathcal{L}^3).$$

This allows us to transform (4.3) into

$$A^*(x;q) = \mathrm{MT}(x;q) + O(\mathrm{ET}(x;q) + \mathcal{L}^3), \tag{4.4}$$

where

$$\mathrm{MT}(x;q) := \frac{1}{q}\sum_{t|q}\sum_{\substack{b=1\\(b,t)=1}}^{t} S_t(b;x)^3, \quad \mathrm{ET}(x;q) := \frac{\mathcal{L}}{q}\sum_{t|q}\sum_{\substack{b=1\\(b,t)=1}}^{t} |S_t(b;x)|^2.$$

We first consider the error term $\mathrm{ET}(x;q)$. By enlarging the summation and by the Parseval identity we have

$$\sum_{\substack{b=1\\(b,t)=1}}^{t} |S_t(b;x)|^2 \le \sum_{b=1}^{t} |S_t(b;x)|^2 \tag{4.5}$$

$$\le t^{\sharp}\{(p_1,p_2)\ ;\ p_1,p_2 \sim x,\ (p_1p_2,t)=1,\ \overline{p_1} \equiv \overline{p_2} \bmod t\} \ll tx(x/t+1).$$

This shows that the first error term in (4.4) satisfies

$$\mathrm{ET}(x;q) \ll q^{-1}x(x+q)\tau(q)\mathcal{L}. \tag{4.6}$$

We are now concerned with the main term $\mathrm{MT}(x;q)$ in (4.4). We introduce a parameter Δ to be fixed later to control the size of t. We then have

$$\mathrm{MT}(x;q) = \mathrm{MT}_{\le\Delta}(x;q) + \mathrm{MT}_{>\Delta}(x;q),$$

where

$$\mathrm{MT}_{\le\Delta}(x;q) := \frac{1}{q}\sum_{\substack{t|q\\t\le\Delta}}\sum_{\substack{b=1\\(b,t)=1}}^{t} S_t(b;x)^3, \quad \mathrm{MT}_{>\Delta}(x;q) := \frac{1}{q}\sum_{\substack{t|q\\t>\Delta}}\sum_{\substack{b=1\\(b,t)=1}}^{t} S_t(b;x)^3.$$

By (3.13), we directly get

$$\mathrm{MT}_{\le\Delta}(x;q) = \frac{1}{q}\sum_{\substack{t|q\\t\le\Delta}} \frac{\mu(t)}{\varphi(t)^2}\widetilde{\pi}(x)^3 + O\bigg(\frac{1}{q}\sum_{\substack{t|q\\t\le\Delta}}(x^3\mathcal{L}^{-B} + t^4x^3\mathcal{L}^{-3B})\bigg). \tag{4.7}$$

The error term of (4.7) simplifies to

$$\frac{1}{q}\sum_{\substack{t|q\\t\le\Delta}}(x^3\mathcal{L}^{-B} + t^4x^3\mathcal{L}^{-3B}) = O(q^{-1}x^3\Delta\mathcal{L}^{-B} + q^{-1}x^3\Delta^5\mathcal{L}^{-3B}). \tag{4.8}$$

The coefficient of $\widetilde{\pi}(x)^3$ in (4.7) is equal to

$$\frac{1}{q}\sum_{\substack{t|q\\t\le\Delta}} \frac{\mu(t)}{\varphi(t)^2} = \frac{1}{q}\prod_{p|q}\bigg(1 - \frac{1}{(p-1)^2}\bigg) + O(q^{-1}\Delta^{-1}). \tag{4.9}$$

For the term $\mathrm{MT}_{>\Delta}(x;q)$ we use the Parseval identity, as in the proof of (4.5):

$$\begin{aligned}\mathrm{MT}_{>\Delta}(x;q) &\ll \frac{1}{q}\sum_{\substack{t\mid q\\ t>\Delta}}\Big(\max_{(b,t)=1}|S_t(b;x)|\Big)\cdot\Big(\sum_{b=1}^{t}|S_t(b;x)|^2\Big)\\ &\ll \frac{1}{q}\sum_{\substack{t\mid q\\ t>\Delta}}\Big(\max_{(b,t)=1}|S_t(b;x)|\Big)\cdot(tx(x/t+1)).\end{aligned}$$

We apply either Theorem 3.1 for $x^{7/9}<t\le x^{13/12}$ or Theorem 3.2 for $\Delta<t\le x^{7/9}$. The above inequality is transformed into

$$\begin{aligned}\mathrm{MT}_{>\Delta}(x;q) &\ll \frac{x^2}{q}\sum_{\substack{t\mid q\\ \Delta<t\le x^{7/9}}}(\tau(t)^{1/2}t^{-1/2}x\mathcal{L}^2+\tau(t)t^{1/4}x^{4/5}\mathcal{L}^{3/2})\\ &\quad+\frac{x^2}{q}\sum_{\substack{t\mid q\\ x^{7/9}<t<x}}x^{15/16+\varepsilon}+\frac{x}{q}\sum_{\substack{t\mid q\\ t\ge x}}tx^{15/16+\varepsilon}.\end{aligned}$$

Since $(x^{7/9})^{1/4}\cdot x^{4/5}=x^{179/180}$, the above inequality is simplified into

$$\mathrm{MT}_{>\Delta}(x;q)\ll\frac{x^3}{q}\mathcal{L}^2\Big(\sum_{\substack{t\mid q\\ t>\Delta}}\frac{\tau(t)^{1/2}}{t^{1/2}}\Big)+\frac{x^{2+179/180+2\varepsilon}}{q}+x^{31/16+2\varepsilon}. \tag{4.10}$$

We now gather (4.2), (4.4) and (4.6)–(4.10) to finally write

$$\begin{aligned}A(x;q) &= \Big\{\prod_{p\mid q}\Big(1-\frac{1}{(p-1)^2}\Big)+O(\Delta^{-1})\Big\}\frac{\widetilde{\pi}(x)^3}{q}\\ &\quad+O(q^{-1}x(x+q)\tau(q)\mathcal{L})+O(q^{-1}x^3\Delta\mathcal{L}^{-B}+q^{-1}x^3\Delta^5\mathcal{L}^{-3B})\\ &\quad+O\Big(\frac{x^3}{q}\mathcal{L}^2\Big(\sum_{\substack{t\mid q\\ t>\Delta}}\frac{\tau(t)^{1/2}}{t^{1/2}}\Big)+\frac{x^{2+179/180+2\varepsilon}}{q}+x^{31/16+2\varepsilon}\Big).\end{aligned}$$

We now impose $q\le x^{17/16-3\varepsilon}$ and choose $\Delta=\mathcal{L}^A$ and $B=2A+3$. We get

$$A(x;q)=\Big\{\prod_{p\mid q}\Big(1-\frac{1}{(p-1)^2}\Big)+O(\mathcal{L}^{-A})+O\Big(\mathcal{L}^5\Big(\sum_{\substack{t\mid q\\ t>\mathcal{L}^A}}\frac{\tau(t)^{1/2}}{t^{1/2}}\Big)\Big)\Big\}\frac{\widetilde{\pi}(x)^3}{q}.$$

This concludes the proof of Theorem 1.2. ∎

4.2. Proof of Theorem 1.5. We see from (1.5) that it is enough to show that

$$\sum_{x\le q\le x^{14/13-\varepsilon}}\Big|\sharp\{(p_1,p_2,p_3)\in\mathcal{T}(x)\ ;\ A(p_1,p_2,p_3)\equiv 0 \bmod q\} - \prod_{p\mid q}\Big(1-\frac{1}{(p-1)^2}\Big)\frac{\widetilde{\pi}(x)^3}{q}\Big| \ll_B \widetilde{\pi}(x)^3\mathcal{L}^{-B} \tag{4.11}$$

uniformly for $x\ge 2$. Let

$$\eta=\frac{169}{672}\varepsilon.$$

Using the bound (1.6), we estimate the contribution to (4.11) from every (η,x)-bad value of q trivially as $O(x^{3+\eta/3}q^{-1})$. Thus by Corollary 3.4 and partial summation we see that their total contribution to the left part of (4.11) is in $O_B(\widetilde{\pi}(x)^3\mathcal{L}^{-B})$ for any positive constant B.

For (η,x)-good values of q, we see from the proof of Theorem 1.2 in §4.1 that it is enough to estimate $\mathrm{MT}_{>\Delta}(x;q)$. The contribution to $\mathrm{MT}_{>\Delta}(x;q)$ of the $t\le x$ is estimated exactly as before (individually for every q). Thus it remains to show the inequality

$$\sum_{\substack{x\le q\le x^{14/13-\varepsilon}\\ q\ (\eta,x)\text{-good}}}\frac{1}{q}\sum_{\substack{t\mid q\\ t>x}}\sum_{\substack{b=1\\(b,t)=1}}^{t}|S_t(b;x)|^3\ll_B\widetilde{\pi}(x)^3\mathcal{L}^{-B} \tag{4.12}$$

(in fact it is easy to see that the lower limit can be taken to be $x^{17/16-\varepsilon}$ but this does not give any improvements or simplifications).

Recalling that for (η,x)-good values of q we have (3.17), and using the bound (4.5) (which for $t>x$ simplifies as $O(tx)$) we derive

$$\begin{aligned}\sum_{\substack{x\le q\le x^{14/13-\varepsilon}\\ q\ (\eta,x)\text{-good}}}\frac{1}{q}\sum_{\substack{t\mid q\\ t>x}}\sum_{\substack{b=1\\(b,t)=1}}^{t}|S_t(b;x)|^3 &\ll x\sum_{\substack{x\le q\le x^{14/13-\varepsilon}\\ q\ (\eta,x)\text{-good}}}\frac{1}{q}\sum_{\substack{t\mid q\\ t>x}}(t^{3/10}x^{3/5}+t^{1/12}x^{5/6})t^{1+\eta}\\ &\le x\sum_{q\le x^{14/13-\varepsilon}}\tau(q)(q^{3/10}x^{3/5}+q^{1/12}x^{5/6})q^{\eta}\\ &\ll x\sum_{q\le x^{14/13-\varepsilon}}(q^{3/10}x^{3/5}+q^{1/12}x^{5/6})q^{2\eta}\end{aligned}$$

$$\ll x((x^{14/13-\varepsilon})^{13/10}x^{3/5} + (x^{14/13-\varepsilon})^{13/12}x^{5/6})(x^{14/13-\varepsilon})^{2\eta}$$
$$\ll x(x^{2-13\varepsilon/10} + x^{2-13\varepsilon/12})x^{28\eta/13} \ll x^{3-13\varepsilon/12+28\eta/13} = x^{3-13\varepsilon/24}$$

for the above choice of η. Thus (4.12) holds for any B, which concludes the proof of Theorem 1.5. ∎

4.3. Proof of Corollary 1.6. Let $\vartheta \geq 14/13$ be as in the statement of this corollary. We use the so called Chebyshev–Hooley technique. First consider the sum

$$\mathrm{CH}(\mathcal{A}_3(x)) := \sum_{n\in\mathcal{A}_3(x)} \log n = \sum_{p_i\sim x} \log(A(p_1,p_2,p_3)).$$

Since all the elements of $\mathcal{A}_3(x)$ are in $[3x^2, 12x^2]$, we deduce that

$$\mathrm{CH}(\mathcal{A}_3(x)) \sim 2\mathcal{L}\,\widetilde{\pi}(x)^3 \quad (x\to\infty). \tag{4.13}$$

Let

$$X := \widetilde{\pi}(x)^3, \quad Y := x^{14/13-\varepsilon}, \quad Z := x^{\vartheta}.$$

By the identity $\log = \Lambda * \mathbf{1}$ and the notation (4.1) we deduce the decomposition

$$\mathrm{CH}(\mathcal{A}_3(x)) = \Sigma_1 + \Sigma_2 + \Sigma_3 + \Sigma_4, \tag{4.14}$$

where

$$\Sigma_1 := \sum_{q\leq Y} \Lambda(q)A(x;q), \qquad \Sigma_2 := \sum_{\substack{q>Y\\ q\,\text{not prime}}} \Lambda(q)A(x;q),$$
$$\Sigma_3 := \sum_{\substack{Y<q\leq Z\\ q\,\text{prime}}} \Lambda(q)A(x;q), \quad \Sigma_4 := \sum_{\substack{q>Z\\ q\,\text{prime}}} \Lambda(q)A(x;q).$$

Our plan is to get upper bounds on Σ_1, Σ_2 and Σ_3, which together with (4.13) give a lower bound on Σ_4.

Theorem 1.5 easily implies

$$\Sigma_1 \sim \left(\frac{14}{13} - \varepsilon\right) X\mathcal{L} \quad (x\to\infty). \tag{4.15}$$

By (1.6), we obtain

$$\Sigma_2 \ll \sum_{\substack{q>Y\\ q\,\text{not prime}}} \Lambda(q) \sum_{\substack{n\leq 12x^2\\ n\equiv 0 \bmod q}} \rho(n) \ll x^{3+\varepsilon} \sum_{\substack{q>Y\\ q\,\text{not prime}}} \frac{\Lambda(q)}{q},$$

which finally gives

$$\Sigma_2 \ll x^{3-\varepsilon}. \tag{4.16}$$

The most delicate work is to prove a valuable upper bound of Σ_3. In that sum, we are counting the 5-tuplets (p_1,p_2,p_3,p,r) satisfying the inequalities $p_i\sim x$, $Y<p\leq Z$ and the equality $A(p_1,p_2,p_3) = pr$. The smooth weight

$\log p$ is harmless. We reinterpret this counting process as searching for primes in the multiset $A(p_1,p_2,p_3)/r$, when this ratio is an integer. The sieve is well adapted to this situation via Theorem 1.5. However, the above inequalities must be converted into inequalities over the integer variable r. Consider the unweighted subsum of Σ_3 defined by

$$\Sigma_3(P) = \sum_{p\sim P} A(x;p),$$

where P is a number satisfying $Y \le P < Z$. Thus we have

$$\Sigma_3 \le \sum_{0\le k\le K_0} \log(2^{k+1}Y)\Sigma_3(2^kY), \tag{4.17}$$

with

$$K_0 := \lfloor \log(Z/Y)/\log 2 \rfloor.$$

Let $r := A(p_1,p_2,p_3)/p$. Since $p \sim P$ we deduce that

$$\frac{3}{2}x^2P^{-1} \le r \le 12x^2P^{-1}. \tag{4.18}$$

Let $\mathcal{C}^{(r)}$ be the multiset of elements of the form $(A(p_1,p_2,p_3)/r)$ where the p_i satisfy $p_i \sim x$, and r is a fixed integer satisfying (4.18) and dividing $A(p_1,p_2,p_3)$. Let z be a parameter less than x. Then

$$\Sigma_3(P) \le \sum_{r \text{ satisfies (4.18)}} S(\mathcal{C}^{(r)},z), \tag{4.19}$$

where $S(\mathcal{C},z)$ is the sifting function up to the point z, that is, the number of elements of $\mathcal{C}$ with all prime factors greater than z.

To apply sieve methods, we must start from an approximation formula for

$$C_d^{(r)} := \sharp\{a \in \mathcal{C}^{(r)} \,;\, d \,|\, a\},$$

where d is a squarefree positive integer. So we introduce the multiplicative function ω defined by

$$\omega(m) := \prod_{p|m}(1-(p-1)^{-2}),$$

and the error term $R(x;m)$ defined by

$$R(x;m) := A(x;m) - \frac{\omega(m)}{m}X$$

(there is no risk to mistake $\omega(m)$ for the number of distinct prime factors of m). We also have the easy equality

$$C_d^{(r)} = A(x;dr).$$

These considerations show that our approximation formula (see [20, (A_1), p. 205]) naturally is

$$C_d^{(r)} = \frac{\omega(dr)/\omega(r)}{d} X^{(r)} + R(x; dr),$$

with

$$X^{(r)} := \frac{\omega(r)}{r} X.$$

The multiplicative function $d \mapsto \omega(dr)/\omega(r)$ is less than 1, so our sieve problem is linear ($\kappa = 1$; see [20, (A_2), p. 205]). We can apply the classical formulas of linear sieve (see [20, equations (6), (7) & (9), p. 209]) giving, for every $D \geq 1$,

$$S(\mathcal{C}^{(r)}, z) \leq \prod_{p<z} \left(1 - \frac{\omega(pr)/\omega(r)}{p}\right) \times \left(F\left(\frac{\log D}{\log z}\right) + O((\log D)^{-1/3})\right) X^{(r)} + \sum_{d<D} |R(x; dr)|. \tag{4.20}$$

In formula (4.20), the O-symbol is independent of our parameter r, and for our application, we only have to know that $F(s) = 2e^{\gamma} s^{-1}$ when $0 < s \leq 3$.

Actually, we shall sum (4.20) over r satisfying (4.18). We must control the error term of this formula up to some point D, as large as possible. Thus, we consider

$$\mathcal{E}(D) := \sum_{d<D} \sum_{r \leq 12x^2 P^{-1}} |R(x; dr)|.$$

We have

Lemma 4.1. *With the above notation, for $D \leq PYx^{-2}$ we have*

$$\mathcal{E}(D) \ll X\mathcal{L}^{-3}.$$

Proof. Writing $|R(x;q)| = |R(x;q)|^{1/2}|R(x;q)|^{1/2}$, by the Cauchy–Schwarz inequality and Theorem 1.5, with $B = 100$, we have

$$\begin{aligned} \mathcal{E}(D) &\leq \sum_{q \leq 12Y} \tau(q)|R(x;q)| \\ &\leq \Big\{ \sum_{q \leq 12Y} \tau(q)^2 |R(x;q)| \Big\}^{1/2} \Big\{ \sum_{q \leq 12Y} |R(x;q)| \Big\}^{1/2} \\ &\ll \widetilde{\pi}(x)^{3/2} \mathcal{L}^{-50} \Big\{ \sum_{q \leq 12Y} \tau(q)^2 |R(x;q)| \Big\}^{1/2}. \end{aligned} \tag{4.21}$$

By (1.6), the inequality $\tau(km) \leq \tau(k)\tau(m)$ and the classical summation

formulas for the divisor function (and partial summation), we have

$$\begin{aligned}\sum_{q\le 12Y}\tau(q)^2|R(x;q)| &\le \sum_{q\le 12Y}\tau(q)^2\Bigg(\sum_{\substack{n\le 12x^2\\ q\mid n}}\rho(n)+\frac{1}{q}\sum_{n\le 12x^2}\rho(n)\Bigg)\\ &\ll x\mathcal{L}^2\sum_{q\le 12Y}\tau(q)^2\Bigg(\sum_{\substack{n\le 12x^2\\ q\mid n}}\tau(n)+\frac{1}{q}\sum_{n\le 12x^2}\tau(n)\Bigg)\\ &\ll x^3\mathcal{L}^3\sum_{q\le 12Y}\frac{\tau(q)^3}{q}\ll x^3\mathcal{L}^{11}.\end{aligned}$$

Inserting this bound in (4.21) we conclude the proof. ∎

We remark that the weaker bound $\rho(n)\ll x^{1+\varepsilon}$ would have been too weak for our purpose. By (4.19), (4.20) and Lemma 4.1, we get

$$\begin{aligned}\Sigma_3(P)\le{}&(1+\varepsilon)X\sum_{r\text{ satisfies (4.18)}}\frac{\omega(r)}{r}\\ &\times\prod_{p\le z}\Big(1-\frac{\omega(pr)/\omega(r)}{p}\Big)F\Big(\frac{\log(PYx^{-2})}{\log z}\Big),\end{aligned}\tag{4.22}$$

which holds for all $\varepsilon>0$ and all sufficiently large x, and for every $z\le x$.

We now simplify (4.22). First of all, an easy computation gives

$$\begin{aligned}\prod_{p\le z}\Big(1-\frac{\omega(pr)/\omega(r)}{p}\Big)&=\prod_{\substack{p\mid r\\ p\le z}}\frac{1-1/p}{1-\omega(p)/p}\prod_{p\le z}\Big(1-\frac{\omega(p)}{p}\Big)\\ &\le(1+O(z^{-1}))C_0V(z)\prod_{p\mid r}\frac{1-1/p}{1-\omega(p)/p},\end{aligned}$$

where C_0 is the infinite product

$$C_0:=\prod_{p\ge 2}\Big(\frac{1-\omega(p)/p}{1-1/p}\Big),$$

and $V(z)$ is the classical Euler product

$$V(z):=\prod_{p\le z}\Big(1-\frac{1}{p}\Big)\sim\frac{e^{-\gamma}}{\log z}\quad(z\to\infty).$$

If we fix

$$z:=(PYx^{-2})^{1/2},$$

the inequality (4.22) simplifies into

$$\Sigma_3(P) \le \frac{2+\varepsilon}{\log(PYx^{-2})} C_0 X \sum_{r \text{ satisfies (4.18)}} \frac{\nu(r)}{r}, \tag{4.23}$$

where $\nu(r)$ is the multiplicative function

$$\nu(r) = \omega(r) \prod_{p|r} \frac{1-1/p}{1-\omega(p)/p}.$$

Consider the Dirichlet series

$$F(s) := \sum_{r=1}^{\infty} \nu(r) r^{-s}.$$

Writing $F(s)$ as

$$F(s) = \prod_p \left(1 + \frac{\nu(p)}{p^s - 1}\right) = \zeta(s) G(s),$$

we see that $G(s)$ is holomorphic for $\Re s > 1/2$.

By classical methods from complex analysis, essentially based on the computation of the integral $(1/2\pi i) \int F(s+1)(R^s/s)\, ds$ on a vertical line of the complex plane, we see that, as $R \to \infty$,

$$\sum_{r \le R} \frac{\nu(r)}{r} = G(1) \log R + F_0 + O(R^{-\delta_0}), \tag{4.24}$$

where δ_0 is a positive absolute constant, and F_0 is another constant which need not be specified. A standard computation gives the identity

$$C_0 \cdot G(1) = 1.$$

Applying (4.24) twice, we simplify (4.23) into

$$\Sigma_3(P) \le \frac{2+\varepsilon}{\log(PYx^{-2})} X \log 8. \tag{4.25}$$

By (4.17) and (4.25) we obtain

$$\Sigma_3 \le (6+3\varepsilon) \widetilde{\pi}(x)^3 \log 2 \cdot \sum_{0 \le k \le K_0} \frac{\log(2^k Y)}{\log(2^k Y^2 x^{-2})}.$$

Dividing by $\mathcal{L}$, we write

$$\log 2 \cdot \sum_{0 \le k \le K_0} \frac{\log(2^k Y)}{\log(2^k Y^2 x^{-2})} = \mathcal{L} \cdot \frac{\log 2}{\mathcal{L}} \sum_{0 \le k \le K_0} \frac{\frac{\log Y}{\mathcal{L}} + k\frac{\log 2}{\mathcal{L}}}{\frac{\log(Y^2 x^{-2})}{\mathcal{L}} + k\frac{\log 2}{\mathcal{L}}}.$$

The above sum is interpreted as a Riemann sum. Hence, for x sufficiently

large,

$$\Sigma_3 \le (6+4\varepsilon)\widetilde{\pi}(x)^3\mathcal{L}\int_0^{\log(Z/Y)/\mathcal{L}} \frac{t+(\log Y)/\mathcal{L}}{t+(\log(Y^2x^{-2}))/\mathcal{L}}\,dt,$$

which finally gives the inequality

$$\Sigma_3 \le (6+\varepsilon)\widetilde{\pi}(x)^3\bigg(\log(Z/Y)+\log(x^2/Y)\log\bigg[\frac{\log(YZx^{-2})}{\log(Y^2x^{-2})}\bigg]\bigg).$$

Combining this with (4.13)–(4.16), we see that

$$\Sigma_4 \gg \widetilde{\pi}(x)^3$$

if Z satisfies the inequality

$$6\bigg(\log(Z/Y)+\log(x^2/Y)\log\bigg[\frac{\log(YZx^{-2})}{\log(Y^2x^{-2})}\bigg]\bigg) \le \bigg(\frac{12}{13}-\varepsilon\bigg)\mathcal{L}.$$

We check that the choice $Z = x^{\vartheta}$ satisfies this inequality for $\vartheta < \vartheta_0$ and a sufficiently small ε. This completes the proof of Corollary 1.6. ∎

Acknowledgements. The authors are very grateful to Alina Ostafe for her comments, and also to the referee for a very careful reading of the paper.

This work started during a very enjoyable stay by I. S. at the ENS (Paris); the hospitality and support of this institution are gratefully acknowledged. During the preparation of this paper, E. F. was supported by Institut Universitaire de France and I. S. was supported by the Australian Research Council Grant DP1092835.

References

[1] V. Blomer, *Ternary quadratic forms, and sums of three squares with restricted variables*, in: Anatomy of Integers, CRM Proc. Lecture Notes 46, Amer. Math. Soc., 2008, 1–17.

[2] V. Blomer and J. Brüdern, *A three squares theorem with almost primes*, Bull. London Math. Soc. 37 (2005), 507–513.

[3] J. Bourgain, *More on the sum-product phenomenon in prime fields and its applications*, Int. J. Number Theory 1 (2005), 1–32.

[4] H. Davenport, *Multiplicative Number Theory*, 2nd ed., Grad. Texts in Math. 74, Springer, 1980.

[5] É. Fouvry et Ph. Michel, *Sur certaines sommes d'exponentielles sur les nombres premiers*, Ann. Sci. École Norm. Sup. (4) 31 (1998), 93–130.

[6] J. B. Friedlander and H. Iwaniec, *Incomplete Kloosterman sums and a divisor problem*, Ann. of Math. 121 (1985), 319–350.

[7] M. Z. Garaev, *An estimate of Kloosterman sums with prime numbers and application*, Mat. Zametki 88 (2010), 365–373 (in Russian).

[8] G. Greaves, *A weighted sieve of Brun's type*, Acta Arith. 40 (1982), 297–332.

[9] —, *Sieves in Number Theory*, Ergeb. Math. Grenzgeb. 43, Springer, 2001.

[10] H. Halberstam and H.-E. Richert, *Sieve Methods*, London Math. Soc. Monogr. 4, Academic Press, 1974.
[11] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 4th ed., Clarendon Press, 1960.
[12] G. Harman and A. Kumchev, *On sums of squares of primes. II*, J. Number Theory 130 (2010), 1969–2002.
[13] D. R. Heath-Brown, *Almost-primes in arithmetic progressions and short intervals*, Math. Proc. Cambridge Philos. Soc. 83 (1978), 357–375.
[14] —, *The density of rational points on Cayley's cubic surface*, Proc. Session in Analytic Number Theory and Diophantine Equations, Bonner Math. Schriften 360, Univ. Bonn, 2003, 33 pp.
[15] C. Hooley, *Applications of Sieve Methods to the Theory of Numbers*, Cambridge Tracts in Math. 70, Cambridge Univ. Press, 1976.
[16] L. K. Hua, *Some results in the additive prime-number theory*, Quart. J. Math. (Oxford) 9 (1938), 68–80.
[17] —, *Additive Theory of Prime Numbers*, Transl. Math. Monogr. 13, Amer. Math. Soc., 1965.
[18] H. Iwaniec, *The half dimensional sieve*, Acta Arith. 29 (1976), 69–95.
[19] —, *Rosser's sieve*, ibid. 36 (1980), 171–202.
[20] —, *Rosser's sieve—bilinear forms of the remainder terms—some applications*, in: Recent Progress in Analytic Number Theory, Vol. 1 (Durham, 1979), Academic Press, 1981, 203–230.
[21] S. V. Konyagin, *Estimates for trigonometric sums over subgroups and for Gauss sums*, in: IV Internat. Conf. "Modern Problems of Number Theory and Its Applications": Current Problems, Part III, Mech.–Math. Faculty, Moscow Lomonosov State Univ., 2002, 86–114 (in Russian).
[22] J. Liu and P. Sarnak, *Integral points on quadrics in three variables whose coordinates have few prime factors*, Israel J. Math. 178 (2010), 393–426.

Étienne Fouvry
Laboratoire de Mathématique
UMR 8628
Université Paris-Sud
F-91405 Orsay, France
and
CNRS
F-91405 Orsay, France
E-mail: Etienne.Fouvry@math.u-psud.fr

Igor E. Shparlinski
Department of Computing
Macquarie University
Sydney, NSW 2109, Australia
E-mail: Igor.Shparlinski@mq.edu.au

Received on 23.11.2010
and in revised form on 16.2.2011 (6559)